

ERIC E. LYNCH, State Bar No. 025049
RYAN G. PIERCE, State Bar No. 025688
MECKLER BULGER TILSON MARICK & PEARSON LLP
3101 North Central Avenue, Suite 900
Phoenix, Arizona 85012
Telephone: 602-734-0850
Facsimile: 602-734-0862
E-mail: eric.lynch@mbtlaw.com
E-mail: ryan.pierce@mbtlaw.com

Attorneys for Plaintiff

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

LEISHA REAVES, individually, and on)	Case No.:
behalf of herself and all others similarly)	
situated,)	CLASS ACTION COMPLAINT
)	
Plaintiff,)	
)	Jury Trial Demanded
vs.)	
)	
CABLE ONE, INC., a Delaware)	
Corporation,)	
)	
Defendant.)	
)	

Plaintiff Leisha Reaves (“Plaintiff”), on behalf of herself and all others similarly situated (the “Class” and each a “Class Member”), by and through their attorneys, Meckler Bulger Tilson Marick & Pearson, LLP, as and for Plaintiff’s complaint and demanding trial by jury, allege as follows upon personal knowledge as to themselves and their own acts and observations and, otherwise, upon information and belief based on the investigation of counsel and which Plaintiff believes further investigation and discovery will support with substantial evidence.

NATURE OF THE CASE

1
2 1. In late 2007, Cable One, Inc. (“Cable One” or “Defendant”) began
3 installing spyware devices on its broadband networks. Cable One continued using the
4 spyware devices through early 2008. The devices funneled all users’ Internet
5 communications—inbound and outbound, in their entirety—to a third-party Internet
6 advertisement-serving company, NebuAd.

7 2. NebuAd and Cable One used the intercepted communications to monitor
8 and profile individual users, inject advertisements into the web pages users visited,
9 transmit code that caused undeletable tracking cookies to be installed on users’
10 computers, and forge the “return addresses” of user communications so their tampering
11 would escape the detection of Users’ privacy and security controls.

12 3. Historically, “spyware” is a term that has been applied to software installed
13 on users’ personal computers. The ISP-based spyware provided by NebuAd and deployed
14 by Cable One represented a radical innovation. In the context of Defendant’s role as the
15 trusted conduit for all its users’ Internet communications, this ISP-based spyware created
16 an unprecedented, extraordinarily pervasive ability to monitor users, identify particular
17 individuals, and tamper with their communications and personal computers—even when
18 those users were interacting with websites with which neither Defendant nor NebuAd
19 had any relationship.

20 4. Cable One gave its users no notice of the impending infiltration and
21 provided no opt-out opportunity. Rather, Cable One provided misleading statements in
22 response to Congressional inquiries about its relationship with NebuAd.

23 5. Cable One did it for the money. For a price per customer per month, Cable
24 One exploited its trusted position as a carrier for users’ private communications, selling
25 its unique ability to access users’ Internet traffic and transmit communications to their
26 personal computers. As to the effects of Defendant’s conduct on users’ privacy, their

1 personal computers, and Defendant's quality of service, Defendant left users to fend for
2 themselves. Accordingly, Plaintiff, on behalf of herself and all other similarly situated
3 users, now seeks the relief requested in this complaint.

4 **PARTIES**

5 6. At all times relevant to this complaint, Plaintiff Leisha Reaves was a citizen
6 and resident of Calhoun County, Alabama, was a subscriber to Cable One's broadband
7 Internet services, and therefore a User, as defined herein.

8 7. At all times relevant to this complaint, Cable One was a commercial
9 provider of high-speed, broadband Internet services to customers in approximately 19
10 states, including Alabama. Cable One is a wholly owned subsidiary of the Washington
11 Post Company. At all times relevant to this complaint, Defendant maintained its
12 corporate headquarters in Phoenix, Arizona.

13 a. Defendant provided Internet services to approximately 720,000
14 customer accounts, including Plaintiff, who accessed the Internet using Cable
15 One-supplied cable modems connected to their personal computers. According to
16 its statement to Congress, the NebuAd test was only conducted in Anniston,
17 Alabama, with 14,000 high-speed Internet subscribers, but overall Cable One had
18 approx 720,000 customers in 19 states. Since a given customer account was often
19 utilized for Internet access by multiple consumers, such as members of the
20 account-holder's household, the actual number of consumers in the affected area
21 using Defendant's ISP services ("Users") was much higher than 14,000.

22 b. As an Internet Services Provider ("ISP") providing broadband
23 Internet services to the consuming public, Cable One was a "provider of an
24 electronic communications service" as defined in the Electronic Communications
25 Privacy Act, Title 18, United States Code, Section 2510(15) (the "Wiretap Act").
26

the wrongdoing alleged in this complaint took place in this State; and (c) Defendant is authorized to do business in and has sufficient minimum contacts with this State and/or has otherwise intentionally availed itself of the markets in this State through the promotion, marketing, and sale of its products and/or services in this State, to render the exercise of jurisdiction by this Court permissible under traditional notions of fair play and substantial justice.

12. Venue is proper in this District under Title 28, United States Code, Sections 1391(b) and (c), in that Defendant's corporate office is located in this District, and a substantial portion of the events and conduct giving rise to the violations of law set forth in this complaint took place in this District.

CONDUCT COMPLAINED OF

A. Defendant's Deployment of Appliances

13. An ISP is a conduit. Its job is to provide users with a connection to the Internet so users can communicate with other Internet-connected parties. Through the ISP's services, users browse websites, engage in e-commerce, hold voice-over-Internet-Protocol (VoIP) conversations, exchange e-mail correspondence, instant messages, and "tweets," and otherwise use the ISP's services to conduct all their Internet activities.

14. In or about late 2007 and continuing through early 2008, Cable One entered into an agreement with NebuAd, Inc. ("NebuAd"), a "third party provider of tailored advertising services." Cable One has acknowledged that it engaged NebuAd and participated in serving advertisements to its Users. (See Letter from Philip P. Jimenez to the Hon. John D. Dingell, Chairman, Committee on Energy and Commerce, United States House of Representatives, August 8, 2008, p.2, http://energycommerce.house.gov/Press_110/Responses%20to%20080108%20TI%20Letter/110-ltr.080108responseCABLE001.pdf); (hereinafter, the "Cable One Resp. to Congress".)

1 15. NebuAd agreed to share with Cable One the revenue from serving
2 advertisements to Cable One Users, paying Cable One based on the number of subscriber
3 accounts, per month, whose communications Cable One diverted to the Appliance.

4 16. Defendant's and NebuAd's actions set forth in this complaint were
5 undertaken by Defendant and NebuAd in the performance of their respective obligations
6 under their agreement.

7 17. On NebuAd's website at <http://www.nebuad.com>, it provided the following
8 overview of its business model:

9 Through its unique technology and methodology, industry
10 expertise, and ISP partnerships, NebuAd is leading the industry to
11 a new level of advertising effectiveness. NebuAd combines web-
12 wide consumer activity data with reach into any site on the
Internet. The result is vastly more data and relevance than existing
solutions that are limited to one network or site.

13 18. NebuAd's ad-serving model relied on its gaining direct access to Users'
14 Internet communications en route to and from Users' personal computers. To accomplish
15 this, Defendant licensed and installed the NebuAd Ultra-Transparent Appliance (the
16 "Appliance") from NebuAd and deployed Appliances in Defendant's Anniston broadband
17 service network location.

18 19. Defendant installed the Appliance in its broadband networks beginning in
19 or about late 2007 and continuing through the middle of 2008.

20 20. With NebuAd's cooperation, Defendant deployed the Appliance by
21 physically situating it within Defendant's existing network infrastructure, reconfiguring
22 its network to recognize the Appliance as a network device, and configuring its network
23 connections to funnel all User Internet activity through the Appliance.

24 21. In the operation of the Cable One-NebuAd relationship, Cable One was
25 responsible for installation of the Appliances; maintaining the flow of Users' Internet
26 traffic to the Appliances; and, subsequently, resuming the handling of intercepted

communications by delivering them to their destinations. Cable One supported the continued operation of the Appliances by providing ongoing network environment resources and services.

22. Owing to Cable One's unique position as an ISP for a large consumer population, it was able to divert Internet traffic on a massive scale. Assuming a single User from each of 14,000 customer accounts visited one website per day during a six-month period, the number of diverted incoming and outgoing communications would be approximately 2.5 million.

23. Cable One claimed to have terminated its use of the Appliances in early 2008. (See Cable One Resp. to Congress, p. 3.)

B. Interception and Use of Personally Identifiable Information
Interception of Users' Electronic Communications

24. The scope of Defendant's indiscriminate diversion of Internet traffic to the Appliance encompassed all of its Users' web navigation activity and other Internet transactions, such as file downloads and inbound and outbound messages—all unfiltered, in their entirety. The communicative components of User traffic diverted to the Appliance necessarily included:

a. all communications protocol types, including web communications (http traffic); encrypted web communications (https traffic); e-mail communications, including web-based email communications (e.g., GMail, Hotmail, and Yahoo email account traffic); instant messages; file transfer protocol (ftp) and secure file transfer protocol (ftps) downloads; and voice-over-Internet-Protocol (VoIP) telephony communications;

b. all navigation information, including Users' search terms and the universal resource locators (URLs) identifying websites and Internet addresses accessed by Users;

1 c. Internet Protocol (IP) addresses, which uniquely and persistently
 2 identified Users' specific personal computers, in that, upon information and belief,
 3 Cable One's Users generally leave their cable modems in an always-on state,
 4 causing Users' personal computers to remain linked to unique, "sticky" IP
 5 addresses, much like static IP addresses;

6 d. personally identifying information¹ and substantive content in
 7 communications relating to personal and sensitive matters such as health events,
 8 insurance coverage, financial and e-commerce transactions, financial account
 9 status details, credit reports, political activities and interests, personal
 10 relationships and dating, job searches, and movie rental choices; privileged
 11 correspondence such as marital and attorney-client communications; and
 12 information contained in the financial records of financial institutions, of card
 13 issuers, as defined in Title 15, United States Code, Section 1602(n), and from the
 14 files of consumer reporting agencies on consumers, as defined in the Fair Credit
 15 Reporting Act, Title 15, United States Code, Section 1681, et seq.; and

16 e. information to, from, and about children under the age of 13.

17
 18 ¹ The Federal Trade Commission has defined "personally identifiable information" or "personal
 19 information" as:

20 individually identifiable information from or about an individual [consumer] including,
 21 but not limited to: (a) a first and last name; (b) a home or other physical address,
 22 including street name and name of city or town; (c) an email address or other online
 23 contact information, such as an instant messaging user identifier or a screen name that
 reveals an individual's email address; (d) a telephone number; (e) a Social Security
 Number; (f) a persistent identifier, such as a customer number held in a "cookie" or
 processor serial number, that is combined with other available data that identifies an
 individual; or (g) any information that is combined with any of (a) through (f) above.

24 *In the Matter of Microsoft Corporation*, Federal Trade Commission, File No. 012 3240, Docket No. C-
 4069, Agreement Containing Consent Order, Aug. 8, 2002, pp. 2-3, [http://www.ftc.gov/os/caselist/](http://www.ftc.gov/os/caselist/0123240/microsoftagree.pdf)
 25 [0123240/microsoftagree.pdf](http://www.ftc.gov/os/caselist/0123240/microsoftagree.pdf); accord *In the Matter of Eli Lilly and Company*, Assurance of Voluntary
 Compliance and Discontinuance, Attorneys General of the States of California, Connecticut, Idaho, Iowa,
 26 Massachusetts, New Jersey, New York, and Vermont, p. 7 n.3, [http://supplierportal.lilly.com/Home/Mul-](http://supplierportal.lilly.com/Home/Multi-State_Order.pdf)
[ti_State_Order.pdf](http://epic.org/privacy/medical/lillyagreement.pdf) and <http://epic.org/privacy/medical/lillyagreement.pdf>.)

1 25. Cable One implicitly admitted it diverted unfiltered Internet traffic to
2 NebuAd—that is, Internet traffic containing personally identifiable information as well as
3 https traffic, web mail, email, instant messages, and VolP conversations—when Cable
4 One told a United States Congressional committee that “no raw data linked to identifiable
5 individuals was stored.” (See Cable One Resp. to Congress, p. 2.) Such an assurance
6 would have been meaningful only if NebuAd was, in fact, receiving unfiltered data from
7 Defendant.

8 26. NebuAd confirmed that it received unfiltered Internet traffic when it stated
9 in Congressional testimony that “the NebuAd service constructs anonymous inferences
10 about the user's level of qualification for a predefined set of market segment categories,
11 and then discards the raw data that was used to create or update a user's anonymous
12 profile.” (See Testimony of Bob Dykes, CEO, NebuAd, Inc., Senate Committee on
13 Commerce, Science and Transportation, “Privacy Implications of Online Advertising,”
14 July 9, 2008, p. 6, [http://commerce.senate.gov/public/_files/RobertDykesNebuAdOnline-](http://commerce.senate.gov/public/_files/RobertDykesNebuAdOnline-PrivacyTestimony.pdf)
15 [PrivacyTestimony.pdf](http://commerce.senate.gov/public/_files/RobertDykesNebuAdOnline-PrivacyTestimony.pdf), emphasis added; hereinafter, “Dykes Senate Testimony.”) Thus,
16 when NebuAd’s CEO testified that “NebuAd's ad optimization and serving system does
17 not collect PII or use information deemed to be sensitive (e.g., information involving a
18 user's financial, sensitive health, or medical matters),” he was not denying NebuAd’s
19 acquisition of such information, merely claiming that NebuAd did not utilize such
20 information to select and deliver advertisements. (See *id.*, p. 4.)

21 27. NebuAd confirmed that it assumed control of User information in
22 testimony before Congress when it described “the NebuAd advertising service—part of
23 which is co-located with, but operates separate and apart from, an ISP’s facilities.” (See
24 Testimony of Bob Dykes, CEO, NebuAd, Inc., House Subcommittee on
25 Telecommunications and the Internet, “What Your Broadband Provider Knows about
26 Your Web Use: Deep Packet Inspection and Communications Law and Policies,” July 17,

1 2008, p. 4, [http://energycommerce.house.gov/images/stories/Documents/Hear-](http://energycommerce.house.gov/images/stories/Documents/Hearings/PDF/Testimony/TI/110-ti-hrg.071708.Dykes-testimony.pdf)
2 [ings/PDF/Testimony/TI/110-ti-hrg.071708.Dykes-testimony.pdf](http://energycommerce.house.gov/images/stories/Documents/Hearings/PDF/Testimony/TI/110-ti-hrg.071708.Dykes-testimony.pdf); hereinafter, “Dykes
3 House Testimony.”)

4 28. In light of the foregoing admissions, Cable One misrepresented the content
5 of User traffic it diverted to NebuAd when it represented to a Congressional committee
6 that NebuAd collected no personally identifiable information. (See Cable One Resp. to
7 Congress, p. 2.)

8 29. In light of the foregoing:

9 a. The Appliance was a device used to acquire the “contents” of
10 communications, as that term is defined in the Wiretap Act, Title 18, United States
11 Code, Section 2510(8), in that Defendant used the Appliance to divert and transfer
12 the substance, purport, and meaning of the communications to the Appliance.
13 Therefore, the Appliance was used to “intercept” the contents of electronic
14 communications, as that term is defined in the Wiretap Act, Title 18, United States
15 Code, Section 2510(4);

16 b. Each of the Defendant’s networks or network segments
17 incorporating the Appliance into its routine operations was a device and apparatus
18 that could be and was used to intercept, retain, and transcribe in-transit electronic
19 communications and was therefore an “electronic, mechanical, or other device” as
20 defined in the Wiretap Act, Title 18, United States Code, Section 2510(5).

21 c. Likewise, each Appliance was itself a device and apparatus that
22 could be and was used to intercept, retain, and transcribe in-transit electronic
23 communications and was therefore an “electronic, mechanical, or other device” as
24 defined in the Wiretap Act, Title 18, United States Code, Section 2510(6).

25 30. Neither Defendant nor NebuAd were the originator or recipient of the User
26 communications traversing Defendant’s networks and, as further detailed in section I. E,

1 “Defendant’s Deception and Lack of Authorization,” below, neither Defendant nor
2 NebuAd were authorized to intercept and read the contents of Users’ communications.
3 Therefore, neither Defendant nor NebuAd were a “party” to Users’ electronic
4 communications, as that term is used in the Wiretap Act, Title 18, United States Code,
5 Section 2511(2)(d).

6 31. Defendant’s interception and eavesdropping was intentional and knowing
7 in that it was undertaken by Defendant in the performance of Cable One’s agreement
8 with NebuAd and accomplished with instrumentalities that included the Appliance and
9 Defendant’s networks installed and configured specifically to perform interception and
10 eavesdropping.

11 **Tracking and Profiling of Individually Identified Users**

12 32. Regardless of whether NebuAd eventually discarded the personally
13 identified content in Users’ “raw data,” it identified individual users and maintained
14 behavioral profiles on them. NebuAd’s profiles were linked not just to individual
15 personal computers, but to the particular users, themselves.

16 33. To obtain information for NebuAd’s behavioral profiles of Users, the
17 Appliance included deep packet inspection (“DPI”) functions that read and analyzed
18 Users’ communications. DPI software enables a party to read the contents OSI layers 6
19 and 7 of the data packets comprising an Internet communication—which is to say that
20 DPI looks past the “envelope” and “handling instructions” layers of an Internet
21 communication and drills down to transcribe the payload—the actual substance intended
22 to be read by the recipient of the communications.

23 34. In addition, despite NebuAd’s claim that “[t]here is no connection or link
24 between the ISP’s registration data systems and NebuAd” (see Dykes Senate Testimony,
25 p. 7), NebuAd’s user profiles included Users’ five-digit zip codes, which it either deduced
26 from Users’ Internet communications or received from Defendant.

1 35. Through NebuAd's identification of individual Users and Defendant's
2 interception of all of its Users' Internet communications, NebuAd could claim, "[W]e're
3 able to get a 360-degree, multidimensional view over a long period of time of all the
4 pages users visit." Behaviorial Insider, Nov. 14, 2007, [http://publications.mediapost.com/-](http://publications.mediapost.com/-index.cfm?fuseaction=Articles.showArticle&art_aid=71020)
5 [index.cfm?fuseaction=Articles.showArticle&art_aid=71020](http://publications.mediapost.com/-index.cfm?fuseaction=Articles.showArticle&art_aid=71020).

6 36. The relationship between Cable One and NebuAd represented an
7 unprecedented and extraordinarily pervasive ability to locate and monitor Users and—as
8 discussed below in section C., "Tampering with User Communications and
9 Computers"—control Users' communications in all of their Internet activities. This
10 ability to identify individuals and intervene in their communications extended to Users'
11 interactions with websites with which neither Defendant nor NebuAd had any
12 relationship.

13 37. The unique and persistent identifiers NebuAd used to track Users and link
14 their online behavior to its profiles constituted personally identifying information, just as
15 a telephone number constitutes personally identifying information used to contact an
16 individual, a street address constitutes personally identifying information used to find or
17 correspond with persons residing at that address, or a global positioning system (GPS)
18 signal constitutes personally identifying information used to locate the GPS device user
19 while in transit. Therefore, Cable One's statement to a Congressional committee that
20 NebuAd used no personally identifiable information was a misrepresentation. (See Cable
21 One Resp. to Congress, p. 2.)

22 **C. Tampering with User Communications and Computers**

23 38. NebuAd and the Appliance used DPI not only to read the contents of Users'
24 communications, but to alter the contents, load the communications with atypically
25 persistent tracking cookies, and forge components of the communications to evade Users'
26

1 security and privacy controls when Defendant ultimately delivered the communications
2 to Users, as follows:

3 a. For a communication en route to a User, if NebuAd identified the
4 opportunity to serve a targeted advertisement, the Appliance inserted the
5 advertisement into the web page being downloaded for display to the User.

6 b. The Appliance also inserted Javascript program code to be executed
7 on the User's personal computer. Upon reaching Users' personal computers, the
8 code forced Users' computers to download cookies from a NebuAd division.
9 Causing Users' computers to contact a third-party website not authorized by the
10 original web page the User downloaded violates Internet Engineering Task Force
11 (IETF) standards designed to maintain the security and integrity of Internet
12 communications. Further, the cookies that the code caused to be deposited on
13 Users' computers were no ordinary cookies that Users could manage with their
14 privacy controls. They were super-persistent cookies that, if removed, simply
15 reappeared. NebuAd's CEO alluded to this fact in testimony before Congress
16 when he stated, "NebuAd has enhanced the industry-standard opt-out "cookie"
17 based system with the use of proprietary techniques. This enables the opt-out to be
18 more persistent." (Dykes Senate Testimony, p. 4 n.4.)

19 c. The Appliance forged the "envelope" of the altered communication
20 to make the communication appear to the User's personal computer as if it were
21 the authentic and unaltered web page the User had requested, thus escaping
22 detection by Users' security controls designed to protect against unauthorized
23 third-party content.

24 d. Cable One then delivered the altered, loaded, forged
25 communications to the User's personal computer.
26

1 39. The Appliance's functions were consistent with NebuAd's March 30, 2007
2 patent application for "[a] network device for monitoring data traffic between a client
3 device and a server device," which stated:

4 The data packets exchanged between a computer and a website
5 being visited are altered or modified in such a way that the head of
6 the packets remains largely intact while the payloads of the packets
 are changed to suit the need.

7 (See U.S. Patent Application No. 11693719, "Network device for monitoring and
8 modifying network traffic between an end user and a content provider," filed Mar. 30,
9 2007, Abstract, Summary ¶¶ 9-10, Claims ¶¶ 4, 8, 12-14, 16; see also U.S. Patent
10 Application No. 11759157, "Method and system for inserting targeted data in available
11 spaces of a webpage," filed June 6, 2007; U.S. Patent Application No. 11759179,
12 "Network device for embedding data in a data packet sequence," filed June 6, 2007; U.S.
13 Patent Application No. 11759187, "Network devices for replacing an advertisement with
14 another advertisement," filed June 6, 2007.)

15 40. The content modification, forgery, and tracking code behavior of the
16 Appliance implemented by Cable One was independently documented in "NebuAd and
17 Partner ISPs: Wiretapping, Forgery and Browser Hijacking" by Robert M. Topolski, co-
18 published by Free Press and Public Knowledge, June 18, 2008,
19 http://www.freepress.net/files/NebuAd_Report.pdf; [http://www.publicknowledge.org/pdf/](http://www.publicknowledge.org/pdf/nebuad-report-20080618.pdf)
20 [nebuad-report-20080618.pdf](http://www.publicknowledge.org/pdf/nebuad-report-20080618.pdf).

21 41. As further detailed in section I. E, "Defendant's Deception and Lack of
22 Authorization," Cable One did not have authority to access Users' personal computers
23 and/or Cable One exceeded what authority they had to access Users' personal computers
24 in that Cable One was not authorized by its Users to transmit altered and forged
25 communications that avoided detection and rejection by Users' security controls and that
26

1 caused the transmission and execution of code that defeated Users' privacy and security
2 management tools.

3 42. Cable One's access of Users' personal computers was knowing and
4 intentional and Cable One was aware of and intended the natural and probable
5 consequences of such conduct, inasmuch as Cable One acted in concert with NebuAd
6 and their actions were undertaken pursuant to an agreement between Cable One and
7 NebuAd to engage in just such conduct.

8 43. Cable One knowingly caused the transmission of programs, information,
9 codes, and commands in that Defendant transmitted forged communications designed to
10 avoid detection by Users' security controls, and Defendant transmitted commands and
11 code that created persistent tracking cookies on Users' personal computers, which were
12 protected computers, defeating Users' privacy management tools.

13 **D. Defendant's Abnormal Course of Business and Unnecessary Conduct**

14 44. Defendant's acts alleged in this complaint far exceeded the scope of the
15 "ordinary course of business" as that phrase is used in the Wiretap Act, Title 18, United
16 States Code, Section 2510(5)(a) and the "normal course of [Defendant's] employment
17 while engaged in any activity which is a necessary incident to the rendition of [its]
18 service or to the protection of the rights or property of the provider of that service" as that
19 phrase is used in the Wiretap Act, Title 18, United States Code, Section 2511(2)(a)(i).

20 45. It was not in Defendant's normal course of business to engage in or
21 facilitate User monitoring and behavioral profiling, advertisement selection, and
22 advertisement delivery—whether by inserting ads into web content being downloaded by
23 Users or by any other means.

24 a. Prior to its installation of the NebuAd devices, Cable One's online
25 advertising activity, if any, was limited to its role in the placement of
26 advertisements on its own web pages. As Cable One admitted, "Cable One does

1 not generally tailor or facilitate the tailoring of Internet advertising based on
 2 consumers' Internet search, surfing, or other online activities.” (Cable One Resp.
 3 to Congress, p. 2.)

4 b. Cable One has repeatedly characterized its foray into profiling and
 5 ad distribution with NebuAd as “small-scale” (Cable One Resp. to Congress.)
 6 Since Cable One's termination of its NebuAd relationship, Cable One has been
 7 able to continue providing Internet services to their Users and have not found that
 8 it must engage in online ad-serving to be capable of providing such services.

9 c. Therefore, consumer profiling and ad selection and delivery were
 10 not activities Defendant conducted in the normal course of its business or as
 11 necessarily incident to its rendition of services or protection of rights or property.

12 46. The particular ad-serving activity in which Defendant participated with
 13 NebuAd was a novel ad-serving model, not one in which Defendant participated in the
 14 normal or necessary conduct of its business. As noted by NebuAd CEO Bob Dykes,
 15 NebuAd and its ISP partners adopted this novel model because “ISPs, who have up to
 16 now facilitated but barely participated in online advertising opportunities, can open new
 17 revenue streams that complement advertiser and publisher objectives to maximize
 18 revenue and generate higher revenue-per-subscriber.” Behavioral Insider, Nov. 14, 2007,
 19 [http://publications.mediapost.com/index.cfm?](http://publications.mediapost.com/index.cfm?fuseaction=Articles.showArticle&art_aid=71020)
 20 [fuseaction=Articles.showAr-](http://publications.mediapost.com/index.cfm?fuseaction=Articles.showArticle&art_aid=71020)
 21 [ticle&art_aid=71020](http://publications.mediapost.com/index.cfm?fuseaction=Articles.showArticle&art_aid=71020). Therefore, Cable One's and NebuAd's collaboration was motivated
 22 by the money-making potential of combining Defendant's unique access to its Users'
 23 communications combined with NebuAd's technology and business relationships—not to
 24 provide Cable One's Users the Internet services to which they had subscribed.

25 47. Defendant's use of the Appliance and deep packet inspection technology
 26 was not in its normal course of business or a necessary incident to its rendition of
 services or protection of their rights or property. In the normal course of an ISP's

1 business and as a necessary incident to its need to protect its customers and network
 2 resources and to maintain the availability of its services, an ISP may indeed use tools that
 3 employ DPI. For example, an ISP may use DPI tools to scan Internet communications for
 4 data content that matches recognized types of security threats, such as malicious viruses
 5 and worms.

6 48. In contrast, Cable One subjected Users' communications to deep packet
 7 inspection to identify users, monitor and track their Internet activity, alter the content of
 8 their communications, and forge communications characteristics that bypassed Users'
 9 security and privacy controls and bugged their personal computers. Contrary to Cable
 10 One's representations to Congress (see Cable One Resp. to Congress, p. 3), its activities
 11 were not for the operations support, policy enforcement, or security purposes disclosed in
 12 its Acceptable Use Policy. Cable One used DPI for its own commercial gain,
 13 independent of any normal and necessary activity in providing Internet services to Users,
 14 preserving its rights, or protecting its property.

15 49. The Appliance was spyware² in that it caused and enabled the surreptitious
 16 tracking of Users' Internet activity and transmittal of code that affected Users' control of
 17 their personal computers. However, unlike traditional spyware, which is installed on a
 18 user's computer, the Appliance represented a new breed of ISP-hosted spyware.

23 ² "Spyware" has been defined as

24 any type of software that is surreptitiously installed on a computer and, without the
 25 consent of the user, could collect information from a computer, could allow third parties
 to control remotely the use of a computer, or could facilitate botnet communications.

26 *FTC v. Pricewert*, Case. No. C-09-2407 (RMW) (N.D. Cal.), Order Appointing Temporary Receiver, June
 15, 2009 (Dkt. 38).

50. The Appliance was adware³ in that it caused the display of advertisements to computer users, and which advertisements were other than those authorized by the publishers of the web pages downloaded by users. Again, unlike traditional adware, the ISP-hosted location of the Appliance's represented an adware innovation.

51. Cable One was an adware marketing partner⁴ in that its installation of the Appliance caused the display of advertisements through adware.

52. Spyware and adware hosting and execution and serving as NebuAd's adware marketing partner were not in Defendant's ordinary course of business, were not necessarily incident to Defendant's rendition of Internet connectivity services, and were not necessarily incident to Defendant's protection of rights and property.

E. Defendant's Deception and Lack of Authorization

53. Cable One relied on its Acceptable Use Policy for authorization to engage in NebuAd-related conduct. It did not provide Users with any notice via letter and/or e-mail nor did it provide notice in its privacy policy on its website.

54. At no time did Cable One disclose that it was intercepting and funneling all User communications to NebuAd, including Users' personally identifiable information; enabling a third party to track and profile individually identified Users, anytime and anywhere, and forge communications being transmitted to them; delivering altered and

³ "Adware" has been defined as:

any downloadable software program that displays advertisements to a computer user, including, but not limited to, programs that display pop-up or pop-under advertisements, redirect website or search requests, install toolbars onto Internet browsers or electronic mail clients, or highlight particular keywords or phrases for Internet users as they surf the web.

In the Matter of Priceline.com Incorporated, Assurance of Discontinuance, Attorney General of the State of New York, Jan. 29, 2007, p. 1, http://www.oag.state.ny.us/media_center/2007/jan/adware-scanned-AODs.pdf.

⁴ "Adware marketing partner" has been defined as "any adware company, ad buyer, affiliate, third party distribution partner or other entity that arranges for, purchases, places, or installs the adware program that displays advertising of the products or services . . . through adware." *Id.*

1 forged communications that affected the integrity, performance, and operations of Users'
2 personal computers. Therefore, Defendant's notices were misleading, deceptive, and
3 constituted material omissions.

4 55. In the case of the NebuAd Ultra-Transparent Appliance, "transparent"
5 meant operating in a manner designed to be invisible to both of the authorized parties to
6 an electronic communication. Users had no reasonable means by which they would have
7 become aware that Cable One was diverting their communications to NebuAd.

8 56. Accordingly, Users received no notice of Defendant's conduct alleged in
9 this Complaint, and consequently, could not have obtained any User consent.

10 **F. User Consequences**

11 57. Cable One's interception and inspection of Users' electronic
12 communications and monitoring of identified Users constituted invasions of Users'
13 privacy:

14 a. Cable One's job as an ISP was to provide a secure and confidential
15 conduit for Users' Internet communications, through connectivity services in
16 which in-transit communications are ordinarily transmitted in solitude and
17 seclusion and not ordinarily displayed or available to the general public or third
18 parties.

19 b. Users' Internet communications were confidential communications
20 intended for receipt by particular recipients that did not include Cable One and
21 NebuAd and, as such, were private affairs of Users.

22 c. Users paid Cable One for its services and entrusted them with all
23 their Internet communications—and the communications of Users who were their
24 family members—with the material expectation that Cable One would provide a
25 connectivity setting that would preserve the privacy of their communications, free
26 from unauthorized and improper interception and inspection.

1 d. Cable One had a duty to Users to hold as confidential all
2 information imparted by and linked to individual Users through their
3 communications and Internet navigation.

4 e. Cable One invaded Users' privacy surreptitiously, by installing
5 technology designed to escape user detection, and further hid its intrusions by
6 issuing deceptive and misleading statements to Users and to a Congressional
7 committee inquiring into the privacy consequences of Cable One's relationship
8 with NebuAd.

9 f. Cable One used Users' communications for commercial purposes
10 other than the purposes for which Users' had entrusted those communications to
11 Cable One.

12 g. The degree of Cable One's intrusions encompassed the entire scope
13 of Users' communications, including personal and confidential content and
14 communications to and from minors; all communications types, including
15 HTTPS, web mail, and VoIP traffic; the entire scope of Users' Internet navigation
16 activity; the entirety of Defendant's User base in Calhoun County, Alabama; a
17 duration of at least several months; and many millions of User communications.

18 h. Cable One's motive was to make money by exploiting the trusted
19 role through which it had access to Users' communications.

20 i. Cable One's intrusions continue to affect Users in that their personal
21 information continues to be retained in identity-linked behavioral profiles stored
22 on NebuAd servers.

23 j. Defendant's selfish motives and willingness to exploit its
24 relationships with Users and betray their privacy interests for its own gain would
25 be highly offensive and objectionable to a reasonable person.
26

1 58. Cable One's conduct alleged in this complaint constituted an ongoing
2 course of conduct that harmed Users and caused them to incur financial losses, in that:

3 a. Cable One, which was compensated by NebuAd for its performance
4 under the Cable One-NebuAd agreement, realized significant economic benefits
5 from the interception and modification of communications that belonged to Users
6 and to which Users enjoyed a superior right of ownership.

7 b. As a carrier of messages with no authority to engage in the activities
8 for which NebuAd compensated Cable One, Cable One appropriated
9 compensation to itself for access to Users' information, communications, and
10 personal computers when such compensation rightfully belonged to Users.

11 c. Cable One did so through a novel technology and business model
12 that it implemented in a surreptitious manner and without adequate notice,
13 intentionally deceiving and misleading Users in order to deprive them of the
14 opportunity to realize the economic benefits flowing from the use of their
15 information and computers.

16 d. Therefore, Cable One was unjustly enriched, and Users are entitled
17 to compensation paid or owed to Cable One by NebuAd, or a just and fair portion
18 of such compensation.

19 e. Further, the diminution in the performance levels of Defendant's
20 services caused by its deployment of the Appliances deprived Users of the utility
21 and quality of services for which they had paid, and Users therefore did not
22 receive the full value of paid-for service.

23 f. Further, the invasions of privacy perpetrated by Cable One in
24 providing its services deprived users of the quality and character of service for
25 which they had paid, and Users therefore did not receive the fair value of paid-for
26 service.

1 59. In Defendant's conduct alleged above, including the allegations of section
2 D, "C. Tampering with User Communications and Computers," Defendant's
3 tampering with Users' personal computers and Internet communications caused damage
4 to Users in that:

5 a. Cable One's interception and processing of intercepted
6 communications consumed resources of and diminished the quality and
7 performance of its Internet connectivity services to users.

8 b. Cable One's alterations and forgeries of communications diminished
9 the utility, integrity, and value of such communications.

10 c. The cookie-creating code Cable One transmitted to Users'
11 computers diminished the performance, utility, value, performance, and
12 capabilities of Users' computers.

13 d. The cookie-creating code and communications with forged origins
14 Cable One transmitted to Users' computers controlled and altered the functioning
15 of Users' computers, including by circumventing Users' security and privacy
16 controls.

17 e. Cable One's actions caused Users to expend money, time, and
18 resources investigating and attempting to mitigate their personal computers'
19 diminished performance and investigating and attempting to remove the
20 persistently recurring and unauthorized third-party tracking cookies installed on
21 their computers without notice or consent; and, in the process, diminished Users'
22 productivity.

23 f. Further, these actions interfered with, diminished, and devalued
24 Users' possessory interests in their personal computers and Internet
25 communications, infringed on Users' right to exclude others from unauthorized
26

1 access to their personal computers, and compromised the integrity and ownership
2 of Users' personal computers.

3 g. Therefore, Users were economically damaged by Cable One's
4 conduct.

5 60. Defendant's conduct alleged above, including that alleged in section D, "C.
6 Tampering with User Communications and Computers," constituted
7 interference with and intermeddling with Users' personal property in that:

8 a. Users' personal computers were their personal property.

9 b. Users' Internet communications were their personal property and
10 property in which Users' rights of possession were superior to Defendant's.

11 c. Users' personal computers were designed to be capable of
12 connecting to the Internet, which connection Defendant provided by means of its
13 networks linked to cable modems installed in Users' homes and connected to
14 Users' personal computers, and for which services and equipment Users paid fees
15 to Defendant.

16 d. Through Defendant's interception, alteration, and forgery of
17 communications, Defendant accessed and obtained control over communications
18 sent from User's computers to other Internet-connected parties and those parties'
19 responses.

20 e. Through Defendant's interception and diversion of communications
21 and through its transmission of commands and codes that caused the creation of
22 unusual and persistent cookies, Defendant diminished the utility, value, speed, and
23 capacity of Users' personal computers.

24 f. Through Defendant's forgery of communications components,
25 Defendant disabled and nullified the utility of security detection controls and
26 privacy management tools on Users' personal computers, altering and

1 commandeering control of the functioning of Users' personal computers,
 2 diminishing the capabilities of Users' personal computers, and compromising the
 3 privacy, security, and integrity of Users' personal computers.

4 g. Further, the consequences of this conduct were devaluations of
 5 Users' personal computers and Internet communications; interference with Users'
 6 possessory interests in their personal computers and Internet communications; and
 7 diminutions in Users' productivity in using their personal computers and Internet
 8 communications.

9 h. Defendant's conduct was unauthorized and in excess of its authority
 10 to transmit Users' Internet communications.

11 i. Therefore, Defendant, without Users' consent, interfered with and
 12 intermeddled with Users' personal computers and Internet communications,
 13 harming Users' personal property and diminishing its value, quality, condition,
 14 and utility, and causing real and substantial damage to Users, including the
 15 damages alleged in the preceding paragraph 59.

16 61. Defendant's conduct alleged was knowing and intentional and Defendant
 17 intended the natural and probable consequences of its acts and omissions.

18 **CLASS ALLEGATIONS**

19 62. Plaintiff brings this class action pursuant to Federal Rule of Civil Procedure
 20 23 on behalf of themselves and the following Class:

21 All individuals who were users of Cable One's Internet services and
 22 whose Internet communications traversing Cable One's Internet
 23 services network were diverted to a NebuAd Appliance.

24 63. Plaintiff reserves the right to revise these definitions of the Class based on
 25 facts they learn during discovery.
 26

64. Excluded from the Class are: (i) any Judge or Magistrate presiding over this action, and the court personnel supporting the Judge or Magistrate presiding over this action, and members of their respective families; (ii) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which a Defendant or its parent has a controlling interest and their current or former employees, officers, and directors; (iii) persons who properly execute and file a timely request for exclusion from the Class; and (iv) the legal representatives, successors, or assigns of any such excluded persons.

65. Numerosity: Individual joinder of all members of the Class is impracticable. The Class includes thousands of individuals. Upon information and belief, Class Members can be identified through the electronic records of Defendant.

66. Class Commonality: Common questions of fact and law exist as to all Class Members and predominate over questions affecting only individual Class Members. All Class Members were Users of Defendant during the time that Defendant engaged in the activities alleged in this complaint. All Class Members' Internet communications were diverted, monitored, intercepted, disclosed, divulged, accessed, copied, retained, inspected, analyzed, tampered with, modified, altered, forged, and/or used by Defendant. Common questions for the Class include:

a. how many Users and User communications were the subject of Defendant's conduct herein alleged;

b. what Internet communications protocol types were affected by Defendant's conduct herein alleged;

c. what personally identifying information was included in the intercepted communications;

d. how intercepted communications were used;

1 e. aside from intercepted communications traffic, what User
2 registration, billing, or other User information was disclosed to NebuAd by
3 Defendant;

4 f. what effect deployment of the Appliances had on Defendant's
5 service levels;

6 g. what authority Defendant had to engage in their uses of Users'
7 electronic communications in the context of their deployment of the Appliance
8 and its relationship with NebuAd;

9 h. what User information collected by or as a result of use of the
10 Appliances continues to be retained by Defendant and/or NebuAd;

11 i. whether Defendant tortiously and unjustly enriched itself;

12 j. whether Defendant violated the Wiretap Act, Title 18, United States
13 Code, Section 2510, et seq.;

14 k. whether Plaintiff and Class Members are entitled to damages,
15 injunctive relief, and other equitable relief as a result of the consequences of
16 Defendant's conduct; and

17 l. if so, what is the measure of those damages and the nature of
18 injunctive and other equitable relief.

19 67. Defendant engaged in a common course of conduct giving rise to the legal
20 rights sought to be enforced by the Class Members. Similar or identical statutory and
21 common law violations, business practices, and injuries are involved. Individual
22 questions, if any, pale by comparison to the numerous common questions that dominate.

23 68. The injuries sustained by the Class Members flow, in each instance, from a
24 common nucleus of operative facts. In each case, without authorization, through an
25 ongoing, routinized, and common course of conduct, Defendant deployed the Appliance
26 and caused Class Members' communications to be intercepted; caused Class Members to

1 be monitored, identified, and tracked in their Internet activity; invaded Class Members'
2 privacy; and tampered with their communications and personal computers.

3 69. Typicality: Plaintiff's claims are typical of the claims of other members of
4 the Class, as the Plaintiff and other Class Members were all subjected to Defendant's
5 identical wrongful conduct based upon the same transactions which occurred uniformly
6 in regards to the Plaintiff and to the Class.

7 70. Adequacy: Plaintiff will fairly and adequately protect the interests of the
8 Class. Plaintiff is familiar with the basic facts that form the bases of the proposed Class
9 Members' claims. Plaintiff's interests do not conflict with the interests of the other Class
10 Members that she seeks to represent. Plaintiff has retained counsel competent and
11 experienced in class action litigation and intends to prosecute this action vigorously.
12 Plaintiff's counsel has successfully prosecuted complex actions including consumer
13 protection class actions. Plaintiff and Plaintiff's counsel will fairly and adequately protect
14 the interests of the Class Members.

15 71. Superiority: The class action device is superior to other available means for
16 the fair and efficient adjudication of the claims of Plaintiff and the proposed Class
17 Members. The relief sought per individual member of the Class is small given the burden
18 and expense of individual prosecution of the potentially extensive litigation necessitated
19 by the conduct of Defendant. Furthermore, it would be virtually impossible for the Class
20 Members to seek redress on an individual basis. Even if the Class Members, themselves,
21 could afford such individual litigation, the court system could not.

22 72. Individual litigation of the legal and factual issues raised by the conduct of
23 Defendant would increase delay and expense to all parties and to the court system. The
24 class action device presents far fewer management difficulties and provides the benefits
25 of a single, uniform adjudication, economies of scale and comprehensive supervision by
26 a single court.

1 NebuAd to intercept and endeavor to intercept Plaintiff's and Class Members' electronic
2 communications.

3 77. Defendant's conduct, including that alleged in section A, "Defendant's
4 Deployment of Appliance" and section B, "Interception and Use of Personally
5 Identifiable Information," above, was in violation of Title 18, United States Code,
6 Section 2511(1)(d) in that Defendant used and endeavored to use the contents of
7 Plaintiff's and Class Members' electronic communications, knowing and having reason
8 to know that the information was obtain through interception in violation of Title 18,
9 United States Code Section 2511(1).

10 78. Through Defendant's interception, endeavoring to intercept, use, and
11 endeavoring to use Class Members' electronic communications, their electronic
12 communications were in fact intercepted and intentionally used in violation of Title 18,
13 United States Code, Chapter 119. Accordingly, Class Members are entitled to:

14 a. such preliminary and other equitable or declaratory relief as may be
15 just and proper;

16 b. damages computed as the greater of (i) the sum of the actual
17 damages suffered by Plaintiff and Class Members plus Defendant's profits made
18 through the violative conduct alleged in this complaint; (ii) statutory damages for
19 each Class Member of \$100 a day for each day of violation; or (iii) statutory
20 damages of \$10,000 per User;

21 c. punitive damages; and

22 d. reasonable attorneys' fees and other litigation costs reasonably
23 incurred.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully prays for the following:

- (a) declaring the action to be a proper class action and designating Plaintiff and her counsel as representatives of the Class;
- (b) as applicable to the Class mutatis mutandis, awarding injunctive and equitable relief including, inter alia:
 - (i) prohibiting Defendant from engaging in the acts alleged above;
 - (ii) requiring Defendant to disgorge all of its ill-gotten gains to Plaintiff and the other Class Members, or to whomever the Court deems appropriate.
 - (iii) requiring Defendant to delete all data wrongfully collected and retained through the acts alleged above;
 - (iv) requiring Defendant to provide Plaintiff and the other Class Members a reasonably clear, conspicuous, effective, and permanent means to decline to participate in any data collection activities by means of the Appliance and any similar device, in any present or future iteration, whether connected to NebuAd or any other third party;
 - (v) awarding Plaintiff and Class Members full restitution of all benefits wrongfully acquired by Defendant by means of the wrongful conduct alleged in this complaint; and
 - (vi) ordering an accounting and constructive trust imposed on the data funds, and other assets obtained by unlawful means as alleged above, to avoid dissipation, fraudulent transfers, and concealment of such assets by Defendant;

- 1 (c) for a preliminary and permanent injunction restraining Defendant and
2 Defendant's officers, agents, servants, employees, and attorneys, and those
3 in active concert or participation with any of them from:
- 4 (i) transmitting any information about Plaintiff's or Class Members' ac-
5 tivities on the internet for advertising purposes to any other
6 websites, without fair, clear and conspicuous notice of the intent to
7 transmit information, including a full description of all information
8 potentially and/or actually available for transmission;
- 9 (ii) transmitting any information about Plaintiff's or Class Members'
10 activities on the internet for advertising purposes to any other
11 websites, without fair, clear and conspicuous opportunity to decline
12 the transmittal prior to any transmission of data or information;
- 13 (d) awarding damages, including statutory damages where applicable, to the
14 Class in an amount to be determined at trial;
- 15 (e) awarding Plaintiff reasonable attorney's fees and costs;
- 16 (f) awarding Plaintiff punitive damages
- 17 (g) awarding pre- and post-judgment interest; and
- 18 (h) granting such other and further relief as the Court may deem just and
19 proper.
20
21
22
23
24
25
26

JURY TRIAL DEMAND

Plaintiff requests trial by jury of all claims that may be so tried.

DATED this 10th day of March, 2011.

MECKLER BULGER TILSON MARICK &
PEARSON LLP

By s/ Ryan G. Pierce

ERIC E. LYNCH

RYAN G. PIERCE

Attorneys for Plaintiff

ORIGINAL electronically filed this 10th day of March, 2011, with:

Clerk, US District Court
District of Arizona
401 West Washington
Phoenix, Arizona 85003

s/ Janice Calkins